Entrust Entelligence™ Verification Plug-in 7.0 for Adobe®

User Guide

Document issue: 2.0

Date: October 2004

Entrust®
Securing Digital Identities & Information

Table of contents

About this book

The guide describes

- what Entrust Entelligence™ Verification Plug-in for Adobe® is and why you would use it
- installation information
- how to digitally sign documents
- how to verify one or more digital signatures
- setting options and configuration parameters

For information on public-key infrastructure concepts and the Entrust cryptographic model, refer to the Entrust Authority™ Security Manager documentation.

Typographic conventions

The following typographic conventions appear in this guide:

Table 1: Typographic conventions

Convention	Purpose	Example
Bold text (other than headings)	Indicates graphical user interface elements and wizards	Click **Next** to continue with the installation.
Italicized text	Used for book or document titles	*Entrust Authority™ Roaming Server 6.0 User Guide*
`Courier` type	Indicates installation paths, file names, Windows registry keys, commands, and text you must enter	`entrust.ini`
Angle brackets < >	Indicates variables (text you must replace with your organization's correct values)	By default, Entrust Entelligence Desktop Manager users have an `entrust.ini` file located at `<WINDOWS>\entrust.ini`

Chapter 1

About Entrust Entelligence™ Verification Plug-in for Adobe®

The Entrust Entelligence™ Verification Plug-in 7.0 for Adobe® is a digital signature plug-in for Adobe Acrobat® and Adobe Reader®. Verification Plug-in allows users to digitally sign or encrypt Adobe documents using a Digital ID managed by Entrust or issued by a third-party certification authority (CA). Verification Plug-in also allows users to verify signatures on received documents or decrypt documents secured for them.

When a user signs an Adobe Portable Document Format (PDF) document, that user's private key is accessed using Entrust Entelligence™ Desktop Manager (formerly Entrust/Entelligence) or the Microsoft® Crypto API (CAPI) store on the user's machine. The document is signed with the user's private key, and then the signature (along with the signing certificate and any other certificates within the trust path) is added inside the PDF file containing the signed document. No additional files are created. Visual indications that the PDF has been signed are displayed on and around the document in the Acrobat viewer.

When a user verifies a PDF document, the signature and any certificates within the trust path that were included during signing are retrieved. Revocation lists and additional certificates may be also be retrieved either from the local CAPI store or an accessible LDAP directory, when available. The PDF is verified using the public key in the signer's certificate, and visual indications that the PDF has been verified are displayed on and around the document in the Acrobat viewer.

Using the full edition of the Verification Plug-in for Adobe, PDF encryption is available. This allows a user to locate encryption certificates for one or more intended recipients using Entrust and Adobe Address Books as well as any accessible LDAP directories. The PDF will be encrypted with a one-time document key that is then secured using the encryption certificate of each recipient. The secured document key is included with the PDF when sent to the recipients.

When a user attempts to open an encrypted PDF, the user's private decryption key will be used to access the document key, which subsequently is used to decrypt the PDF.

Chapter 2

System Requirements

The Entrust Entelligence™ Verification Plugin for Adobe® requires the following software:

- Microsoft® Windows® NT, 2000 Professional, or XP Professional
- Microsoft® Internet Explorer 5.5 or later with 128-bit encryption

For users that wish to sign documents:

- Adobe® Acrobat® 6.0 or Adobe® Reader® 6.0 enabled with Reader Extensions®
- Entrust Entelligence™ Desktop Manager (formerly Entrust/Entelligence) 6.1 or later and/or signing keys in the Microsoft CAPI store

For users that wish to verify signed documents:

- Adobe® Acrobat® 6.0 OR
- Adobe® Reader® 6.0

Chapter 3

Getting Started

Installation overview

The Verification Plug-in for Adobe is easy to install. The installer you receive will have been pre-configured by your organization, making the Verification Plug-in for Adobe ready for use upon install.

To install the *Full Edition* of Verification Plug-in for Adobe

1. Verify that either Adobe Acrobat 6.0 or Adobe Reader 6.0 with Reader Extensions has already been installed on your system.
2. If Entrust Entelligence Desktop Manager will be used for applying digital signatures, verify that Entrust Entelligence Desktop Manager 6.1 or later has been installed with a properly configured `entrust.ini` file located in the `C:\winnt` directory.
3. Insert the Verification Plug-in for Adobe CD-ROM to auto-start the installation, or double-click the `Setup.exe` within the CD-ROM to manually start the installation. Verification Plug-in for Adobe will auto-detect installed software and versions and configure itself for use within your Adobe software.

To install the *Verify Only Edition* of Verification Plug-in for Adobe

1. Verify that either Adobe Acrobat 6.0 or Adobe Reader 6.0 has already been installed on your system.
2. Insert the Verification Plug-in for Adobe CD-ROM to auto-start the installation, or double-click the `Setup.exe` within the CD-ROM to manually start the installation. Verification Plug-in for Adobe will auto-detect installed software and versions and configure itself for use within your Adobe software.

Chapter 4

Using Entrust Entelligence™ Verification Plug-in for Adobe®

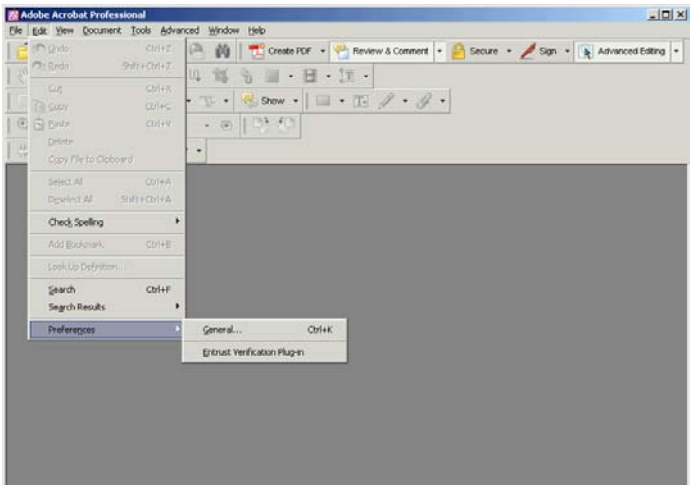
Configuring plug-in options

The Verification Plug-in for Adobe will be pre-configured by your organization so that it is ready for use after installation. Depending on the use of the plug-in, you may need to adjust its configuration over time.

To configure the Verification Plug-in for Adobe

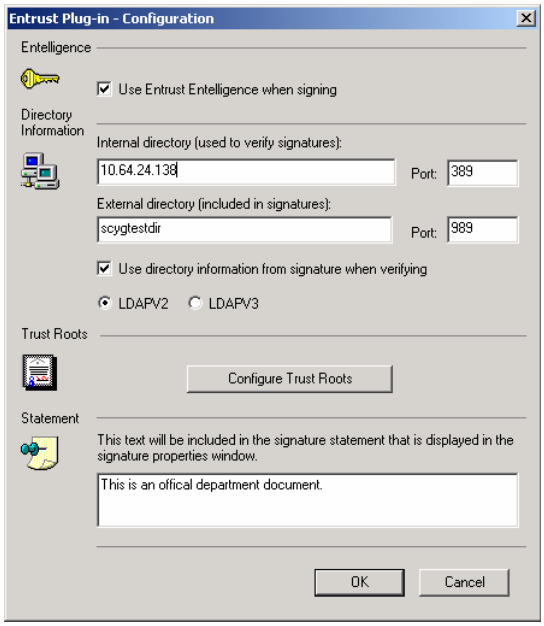
1 Within Adobe Acrobat or Reader, select the **Preferences•Entrust Verification Plug-in** menu item.

Figure 1: Plug-in configuration menu item



2 The **Entrust Plug-in Configuration** dialog will appear.

Figure 2: Plug-in configuration dialog (Full Edition)



The Full Edition of the plug-in contains the following configuration options:

When checked, the **Use Entrust Entelligence when signing** checkbox will cause the plug-in to access the user's Entrust Digital ID through Entrust Entelligence Desktop Manager. This option is only available when Entrust Entelligence Desktop Manager 6.1 or later is installed on the signer's workstation. When not checked, the plug-in will access the user's Digital ID located in the Personal CAPI store on the local system.

The **Internal directory (used to verify signatures)** and **Port** settings contain an IP address, machine name, or fully-qualified domain name and TCP port number of an LDAP directory that will be used when verifying signatures.

The **External directory (included in signatures)** and **Port** settings contain an IP address, machine name, or fully-qualified domain name and TCP port number of an LDAP directory that will be included in signatures applied by the user. This information can be used by the reader to access revocation lists and certificates from the signer's directory during signature verification.

When checked, the **Use directory information from signature when verifying** checkbox will cause the plug-in to utilize directory information included in a signature to locate revocation lists and certificates needed for verification. This setting will override any values set in the **Internal directory (used to verify signatures)** and **Port** settings when directory information is contained in a signature. When no directory information has been included, the **Internal directory (used to verify signatures)** and **Port** settings will be used.

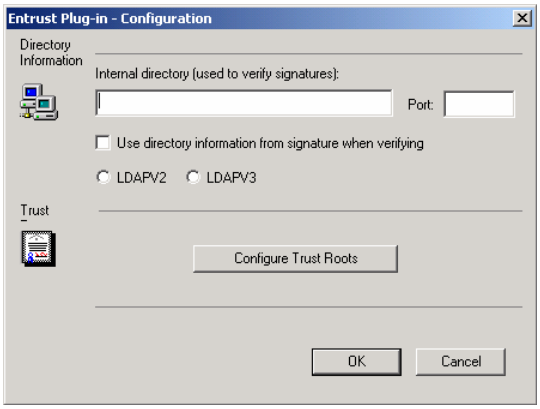
The **LDAPV2** and **LDAPV3** radio buttons allow the user to select which version of the LDAP protocol should be used by the plug-in when trying to retrieve revocation lists and certificates from an LDAP directory. This option is included to maintain support for older directories that may only

support LDAP version 2, however most directory services now support LDAP version 3.

The **Statement** is a text message that will be included with all signatures applied by the user. The organization may choose to use this field to provide a legal or warranty statement regarding the applicability of signatures, or to provide references to more information. When verifying a signature containing a statement, the reader will display the statement field in the signature properties dialog.

The **Configure Trust Roots** button is discussed below.

Figure 3: Plug-in configuration dialog (Verify Only Edition)



The Verify Only Edition of the plug-in contains the following configuration options:

The **Internal directory (used to verify signatures)** and **Port** settings contain an IP address, machine name, or fully-qualified domain name and TCP port number of an LDAP directory that will be used when verifying signatures.

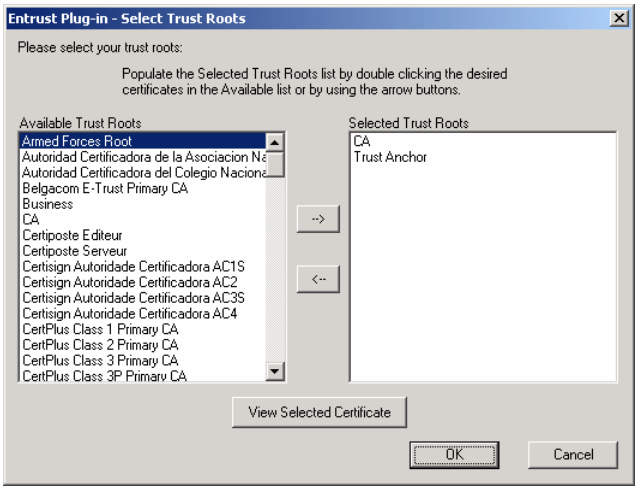
When checked, the **Use directory information from signature when verifying** checkbox will cause the plug-in to utilize directory information included in a signature to locate revocation lists and certificates needed for verification. This setting will override any values set in the **Internal directory (used to verify signatures)** and **Port** settings when directory information is contained in a signature. When no directory information has been included, the **Internal directory (used to verify signatures)** and **Port** settings will be used.

The **LDAPV2** and **LDAPV3** radio buttons allow the user to select which version of the LDAP protocol should be used by the plug-in when trying to retrieve revocation lists and certificates from an LDAP directory. This option is included to maintain support for older directories that may only support LDAP version 2, however most directory services now support LDAP version 3.

The **Select Trust Roots** button displays the **Select Trust Roots** dialog which allows the user to select from one or more self-signed certificates located in the Trusted Root Certification Authorities CAPI store on the local machine in which to place explicit trust. Selecting a trust root means the reader is placing trust in certificates issued by that trust root, and all certificate issuers subordinate to that root. A signature applied by a user who has a certificate issued by a CA that is not a selected trust root or subordinate to one will always fail to verify. The user may highlight a trust root and click

View Selected Certificate to see the details of that trust root to decide whether to select it or not.

Figure 4: Plug-in trust root selection dialog



Signing a PDF Document

The Verification Plug-in for Adobe can add digital signatures to PDF documents (Full Edition of Verification Plug-in for Adobe only). Multiple signatures can be added to a document; however, each new signature constitutes a new revision of the document.

To add a signature to a PDF document:

1 Open Adobe Acrobat.

2 Open the PDF file you wish to sign in Adobe Acrobat.

3 Select the **Sign** button from the toolbar shown in Figure 5. If this is the first signature that will be applied to the document, the dialog in Figure 6 will appear. If the signer chooses to **Certify Document**, a signature will be applied and the user may impose restrictions on further document modification as shown in Figure 7. See the *Adobe Acrobat 6.0 User Guide* for more information on certifying a document. Alternatively, the user can click **Continue Signing** to apply a signature but leave the document unrestricted from further revisioning.

Figure 5: Adobe toolbar

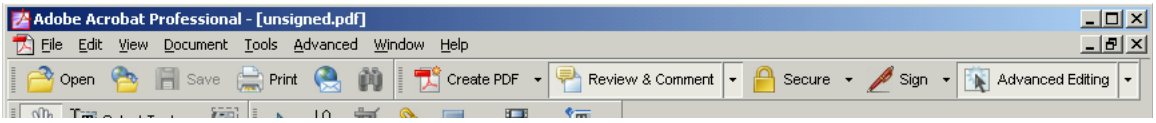
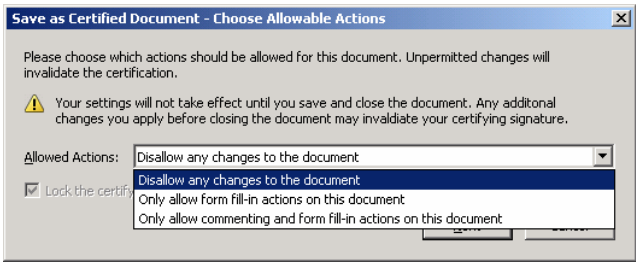


Figure 6: First document signature

Figure 7: Certification restrictions



4 Draw a box on the document in the location you wish the digital signature indication to appear.

Note: The entire document is signed regardless of the location the box is drawn. The location of the box will be used only to display a visual indication that the document has been signed and of its verification status.

---

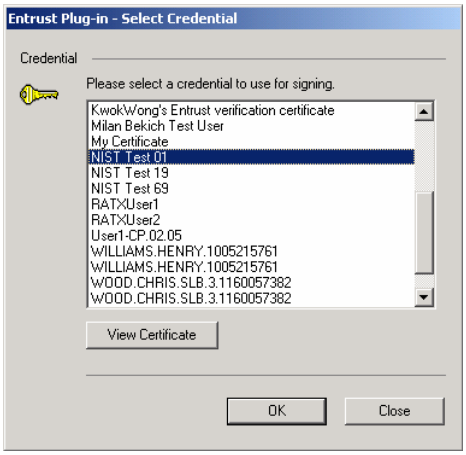
5 If the signer has selected the **Use Entrust Entelligence when signing** configuration option described above, Entrust Entelligence Desktop Manager will be used to apply the digital signature. If the signer has not already logged into Entrust Entelligence Desktop Manager, the **Entrust Login** dialog will appear as shown in Figure 8. The user must

select an Entrust Desktop profile (.epf file), enter their Entrust Roaming user ID, or insert their smart card or hardware token, and enter their Digital ID password.

If the signer has not selected the **Use Entrust Entelligence when signing** configuration option, CAPI will be used to apply the digital signature. The user will see the dialog shown in Figure 9. This dialog lists the Digital IDs found in the Personal CAPI store on the local machine. The user may highlight a Digital ID and click **View Certificate** to verify the Digital ID information before selecting to use it.

Figure 8: Entrust Login dialog

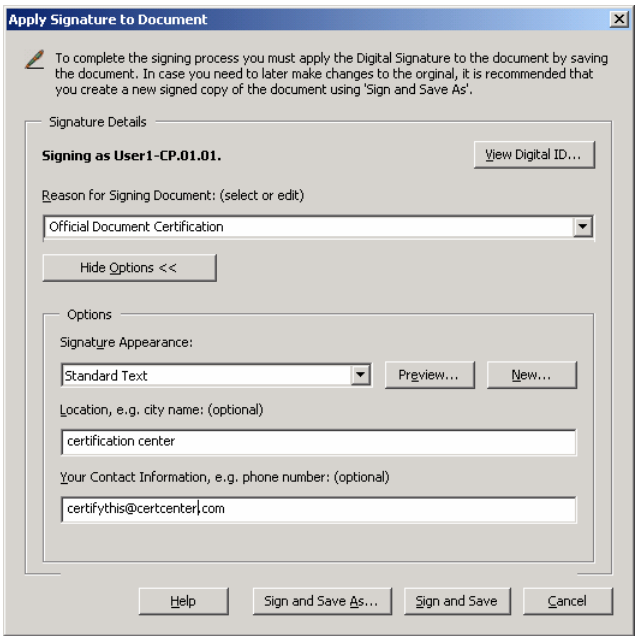
Figure 9: CAPI Digital ID selection



6 After selecting a Digital ID, the user may specify additional signature parameters in the dialog shown in Figure 10. You may select an available reason using the **Reason for Signing Document** pull-down menu or enter a new reason. This entry may be left blank. The **Signature Appearance** option allows the user to specify whether the signature includes a custom graphic logo. The user may also set **Location** and **Contact Information** values to be included with the signature and displayed to the reader when verifying the signature.

When the user has not selected the **Use Entrust Entelligence when signing** configuration option and depending on the security level setting on the user's Digital ID, CAPI may display a dialog prompting the user to enter their Digital ID password to authorize the signing.

Figure 10: CAPI Digital ID selection

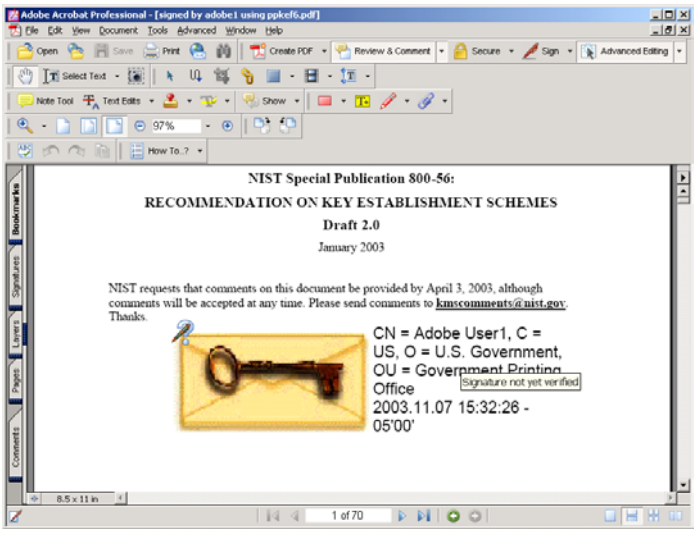


Verifying signatures on a PDF document

The Verification Plugin for Adobe can verify digital signatures that have been added to a PDF document. More than one signature may appear on a document.

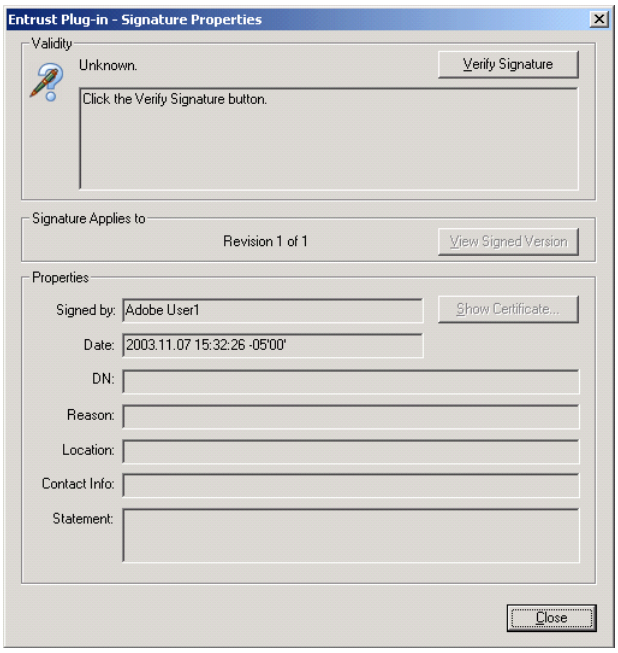
Prior to signature verification, Adobe will display each signature block with a graphical icon as shown in the upper left-hand corner of the signature block of Figure 11. The grey 'question-mark' icon indicates the signature status is undetermined. Note that in this example, the signer has included a custom graphic logo with the signature.

Figure 11: Unverified signature



The reader may right-click on the signature block and select to view the signature **Properties** as shown in Figure 12. The properties dialog reflects that the signature has not yet been verified. The reader may click **Verify Signature** to perform the verification from within the properties dialog, if desired.

Figure 12: Unverified signature properties



To verify all of the signatures on a PDF document:

1 Open Adobe Acrobat or Adobe Reader.

2 Open the PDF file that contains the signatures to be verified.

3 Select the **Tools•Digital Signatures•Verify All Signatures** menu item.

4 Examine each signature's verification status individually.

Understanding Signature Status

The Verification Plug-in for Adobe can return several different results when verifying a signature within a PDF document. The following results may be returned to the reader.

When a signature is valid, the icon and dialog message shown in Figures 13 and 14 will be displayed. A valid signature, symbolized by a green checkmark, indicates that the document has not been modified since signed, the certificate and certificate chain have been processed correctly and end in a selected trust root, each certificate in the chain is valid and not expired, and that a revocation list for each certificate in the chain was obtained and no certificates were revoked.

Note: A signature will only display as fully valid when it has been applied to the most current revision of the PDF document.

Figure 15 shows the properties dialog that appears when the reader clicks **Signature Properties** on the **Signature Validation Status** dialog. The reader may click **Show Certificate** to see the certificate details from the signer's certificate.

Figure 13: Valid signature

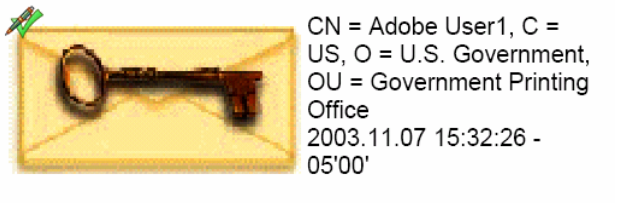
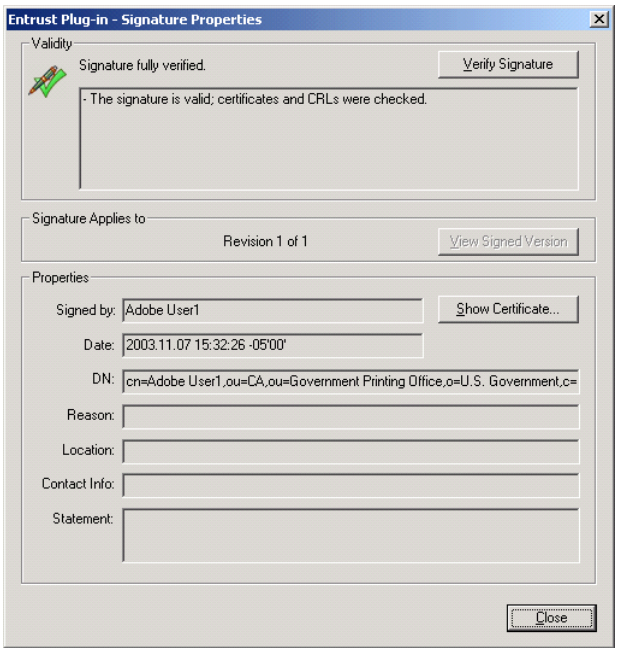


Figure 14: Valid signature dialog

Figure 15: Valid signature properties



When a signature has been applied to a previous revision of the PDF, the Verification Plug-in for Adobe will display the icon and dialog message shown in Figures 16 and 17. In this example, the signer did not include a custom graphic logo with the signature.

When viewing the signature properties on this type of signature, the reader has a new option to click **View Signed Version**. This option shows the reader the revision of the document as it was when this particular signature was applied. The properties dialog, shown in Figure 18, also indicates which revision number the signature was applied to in the lifecycle of the PDF.

Figure 16: Valid signature on previous revision

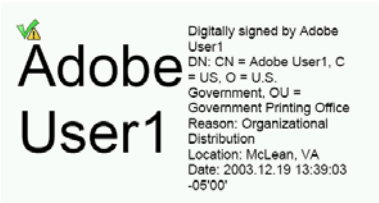
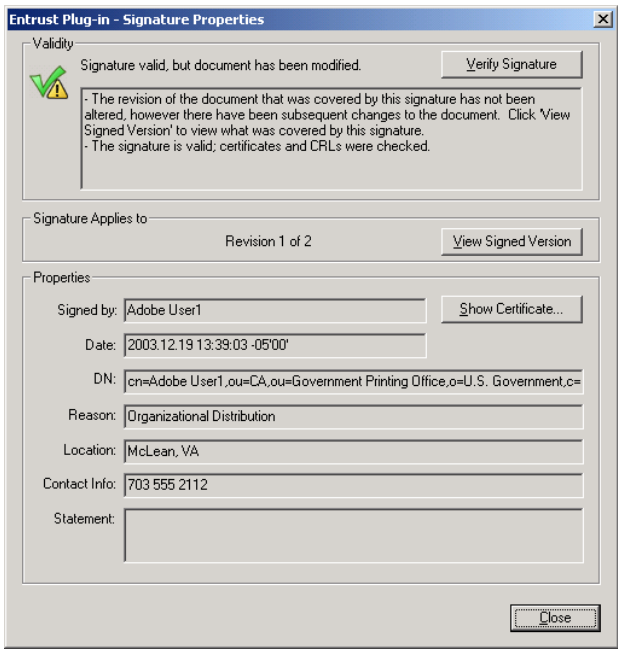


Figure 17: Valid signature on previous revision dialog

Figure 18: Valid signature on previous revision properties



When a signature cannot be verified because the signer's identity is unknown, or certificates and/or revocation lists could not be obtained to validate the signature, but the signature itself is valid (thereby assuring the integrity of the document), the Verification Plug-in for Adobe will display the icon and dialog message shown in Figures 19 and 20. Figure 21 shows the properties dialog for the signature, which reflects the same status information but is more specific about the cause of the failure to verify the signature.

Figure 19: Unverifiable signature

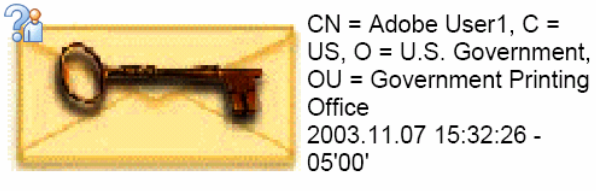
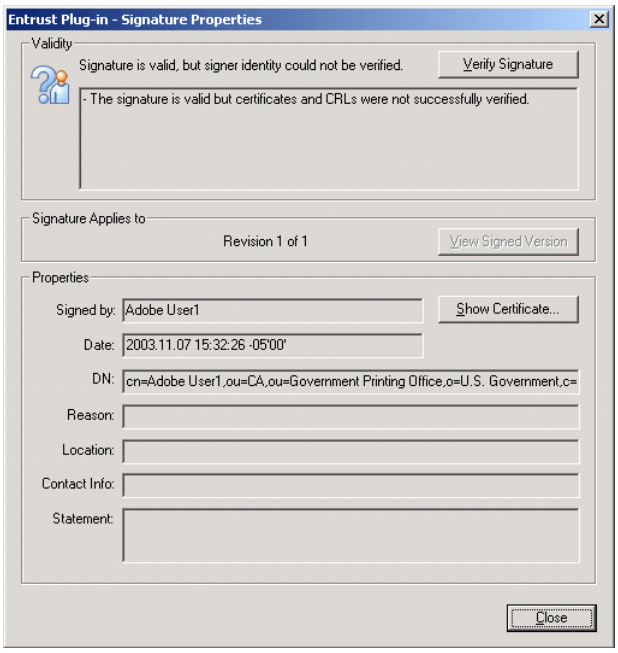


Figure 20: Unverifiable signature dialog

Figure 21: Unverifiable signature properties



When a signature cannot be verified because the signer's identity is unknown, or certificates and/or revocation lists could not be obtained to validate the signature, but the signature itself is valid (thereby assuring the integrity of the document), and the signature applies to a previous revision of the document, the Verification Plug-in for Adobe will display the icon and dialog message shown in Figures 22 and 23.

Figure 24 shows the properties dialog for the signature, which allows the reader to view the revision to which the signature was applied.

Figure 22: Unverifiable signature on previous revision

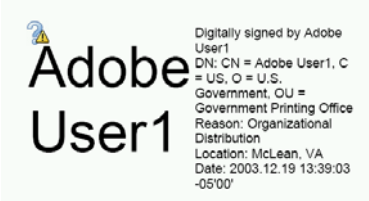
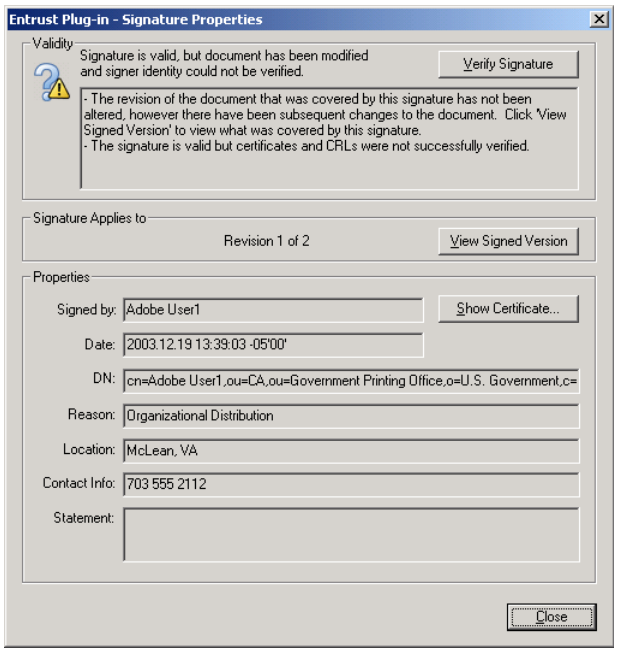


Figure 23: Unverifiable signature on previous revision dialog

Figure 24: Unverifiable signature on previous revision properties



When a signature results in processing a certificate that has expired or been revoked, the Verification Plug-in for Adobe will display the icon and dialog message shown in Figures 25 and 26. Figure 27 shows the properties dialog for the signature, which details the reason for the failure. In the example below, the signer's certificate has been revoked.

Figure 25: Non-trusted signature

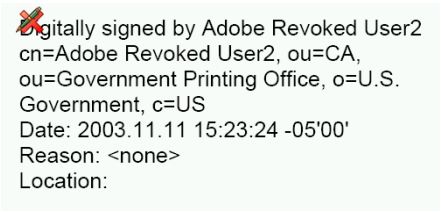
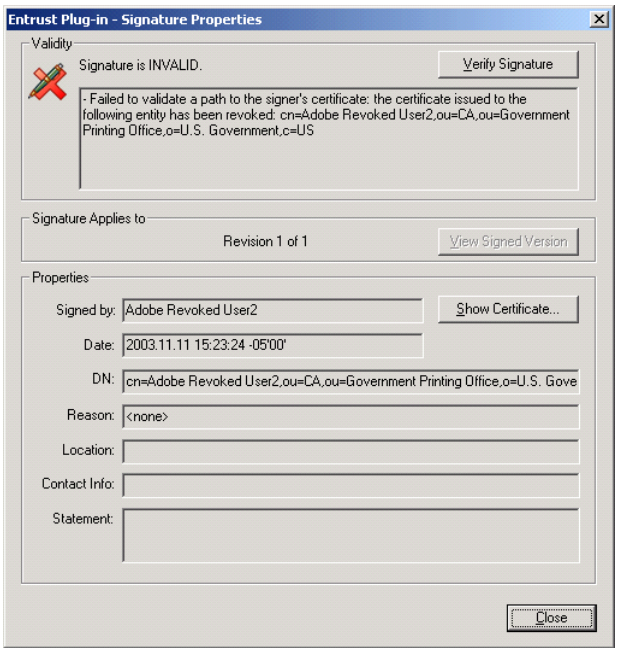


Figure 26: Non-trusted signature dialog

Figure 27: Non-trusted signature properties



When signature verification fails because it is determined that the document has been altered since the signature was applied, the Verification Plug-in for Adobe will display the icon and dialog message shown in Figures 28 and 29 indicating that the signature cannot be trusted. Figure 30 shows the properties dialog for the signature, which details the reason for the failure. In the example below, the document was altered.

Figure 28: Non-trusted signature (alteration)

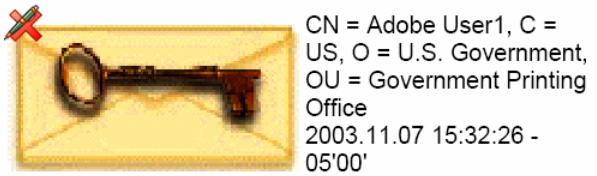
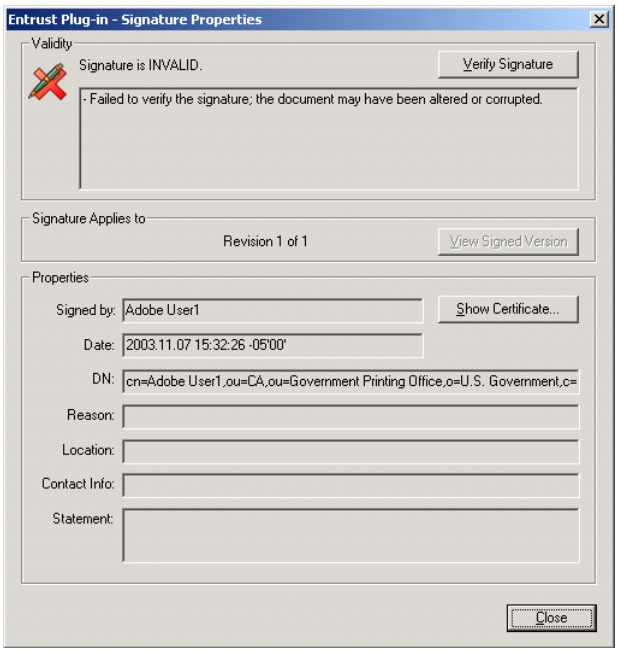


Figure 29: Non-trusted signature (alteration) dialog

Figure 30: Non-trusted signature (alteration) properties

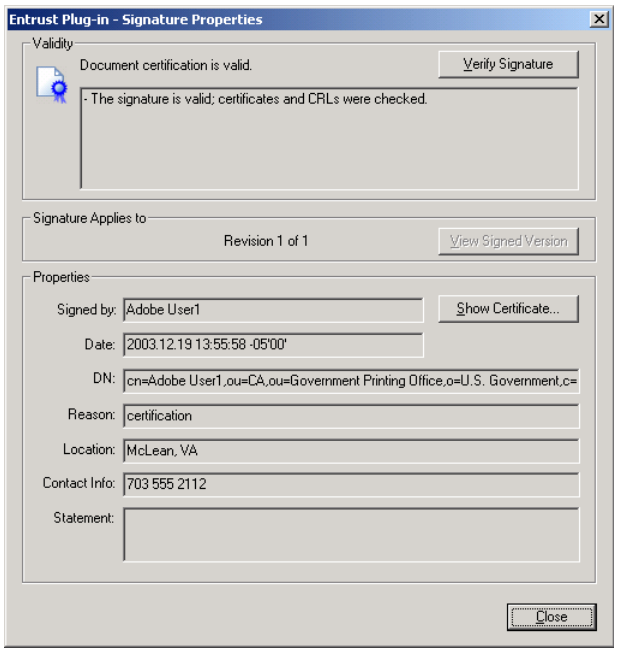


When a certified signature is valid, the icon and dialog message shown in Figures 31 and 32 will be displayed. A certified signature is the only signature that may appear in a certified document and indicates the author or publisher has issued the document with restrictions on how it may be used and has prevented any unauthorized modifications.

Figure 31: Certified signature

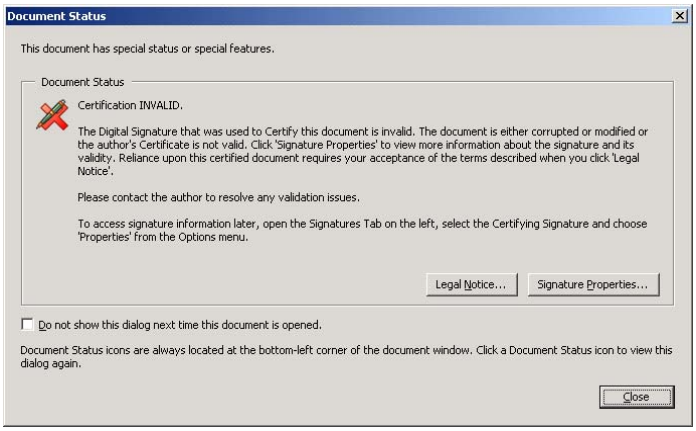
Figure 32: Certified signature dialog

Figure 33: Certified signature properties



Finally, if a certified signature is rendered invalid through document alternation, Verification Plug-in for Adobe displays the dialog shown in Figure 34.

Figure 34: Failed certification signature dialog



Encrypting a PDF Document

The Verification Plug-in for Adobe (Full Edition only) can be used to encrypt a PDF for one or more recipients. This allows users without other secure communications such as secure e-mail to exchange and share sensitive documents with privacy.

Note: Adobe does not allow documents to be both signed and encrypted. Only unsigned documents may be encrypted using Adobe Acrobat.

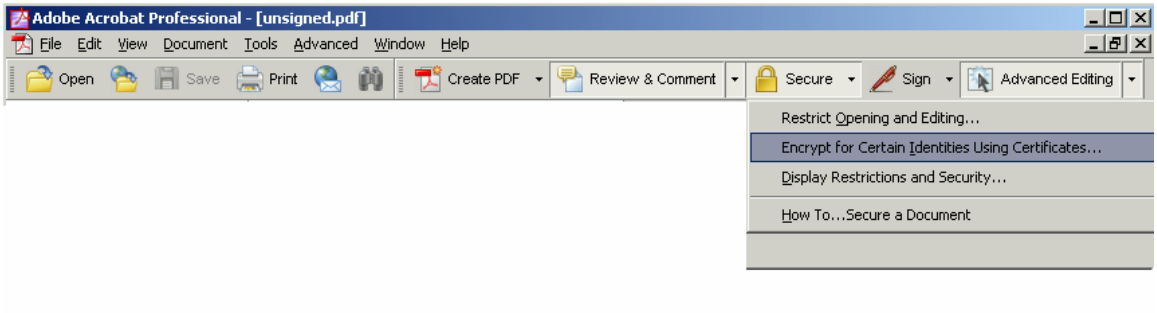
To encrypt a PDF document:

1 Open Adobe Acrobat.

2 Open the PDF file you wish to entrust in Adobe Acrobat.

3 Select the **Secure•Encrypt for Certain Identities Using Certificates** button from the Adobe toolbar shown in Figure 35.

Figure 35: First document signature

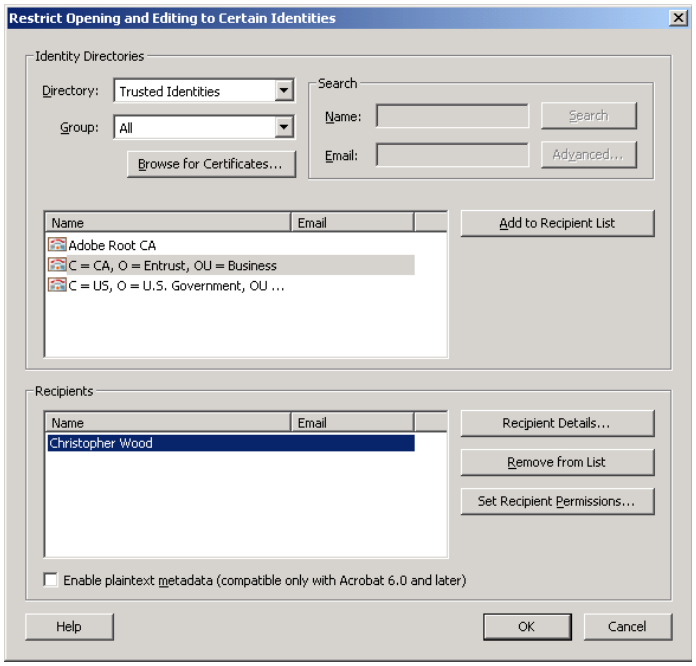


4 If the user has Entrust Entelligence Desktop Manager installed on their system and the user has not already logged into Entrust Entelligence Desktop Manager, the **Entrust Login** dialog will appear as shown in Figure 36. The user must select an Entrust Desktop profile (.epf file), enter their Entrust Roaming user ID, or insert their smart card or hardware token, and enter their Digital ID password.

Figure 36: Entrust Login dialog

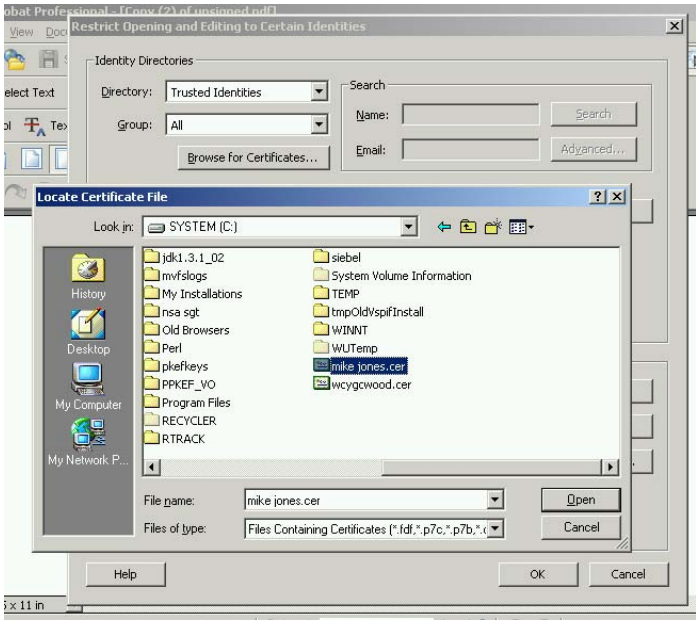
5 The user will be presented with a dialog to select recipients for whom the document will be encrypted. By default, the user is always included in the recipient list to ensure they may open their own document, as shown in Figure 37.

Figure 37: Recipient selection dialog



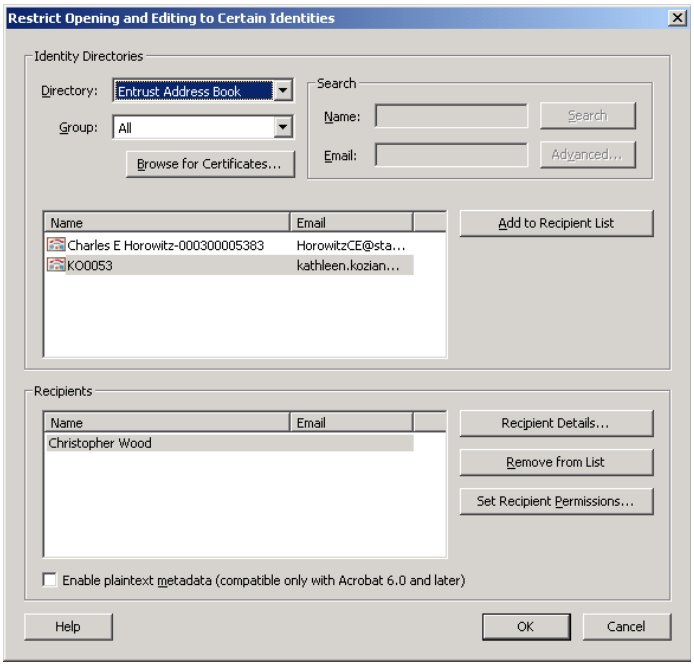
6 Set the **Directory** to `Trusted Identities` and click **Browse for Certificates** to locate certificates within the file system of the workstation as shown in Figure 38.

Figure 38: Trusted identity browsing



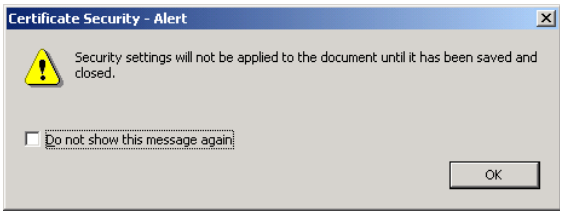
7 Set the **Directory** to `Entrust Address Book` to view a list of recipients within the Entrust Address Book as shown in Figure 39.

Figure 39: Entrust Address Book selection



8 Click **OK** once the selection of recipients is completed. Adobe will present the dialog shown in Figure 40, indicating the document will not be encrypted until it is saved and closed.

Figure 40: Certificate security alert



Decrypting a PDF Document

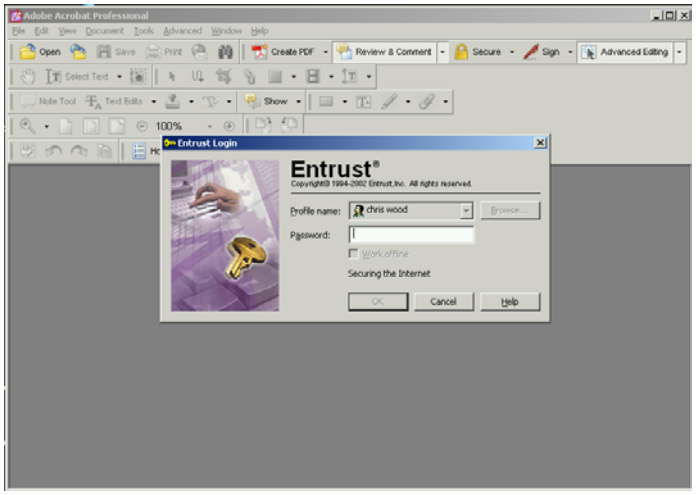
Both Adobe Acrobat and Reader can be used to view encrypted PDF documents. This allows users without other secure communications such as secure e-mail to exchange and share sensitive documents with privacy.

Note: The Full Edition of the Verification Plug-in for Adobe is required for users decrypting PDF documents using a Digital ID accessed through Entrust Entelligence Desktop Manager.

To decrypt a PDF document:

1. Open Adobe Acrobat.
2. Open the PDF file you wish to entrust in Adobe Acrobat.
3. If the user has Entrust Entelligence Desktop Manager installed on their system and the user has not already logged into Entrust Entelligence Desktop Manager, the **Entrust Login** dialog will appear as shown in Figure 41. The user must select an Entrust Desktop profile (.epf file), enter their Entrust Roaming user ID, or insert their smart card or hardware token, and enter their Digital ID password. If the user has a Digital ID accessible through CAPI, they may be prompted by CAPI to enter a password depending on the security assigned to that Digital ID.

Figure 41: Entrust login for decryption



4 If the user fails to activate their Digital ID or is not a selected recipient of the document, the Adobe error message in Figure 42 will appear.

Figure 42: Failed decryption dialog